EVERFOX

DARKREADING

Ten Elements of Insider Risk in Highly Regulated Industries

Insider risk is defined as the "likelihood of harm to an organization due to potential threats coming from the action or inaction of an **insider**, which is someone who has or previously had authorized access or knowledge of organizational resources including people, processes, info, technology or facilities.

Organizations in highly regulated industries like government, healthcare, finance, technology, and energy handle vast amounts of personal data. Should this sensitive data fall into criminal hands, the consequences could be severe, so these organizations face regulatory laws with harsh penalties when security fails.

All organizations should understand insider risks in order to defend themselves. Here are ten elements you should keep in mind regarding threats from within:

1. Malicious vs. Negligent

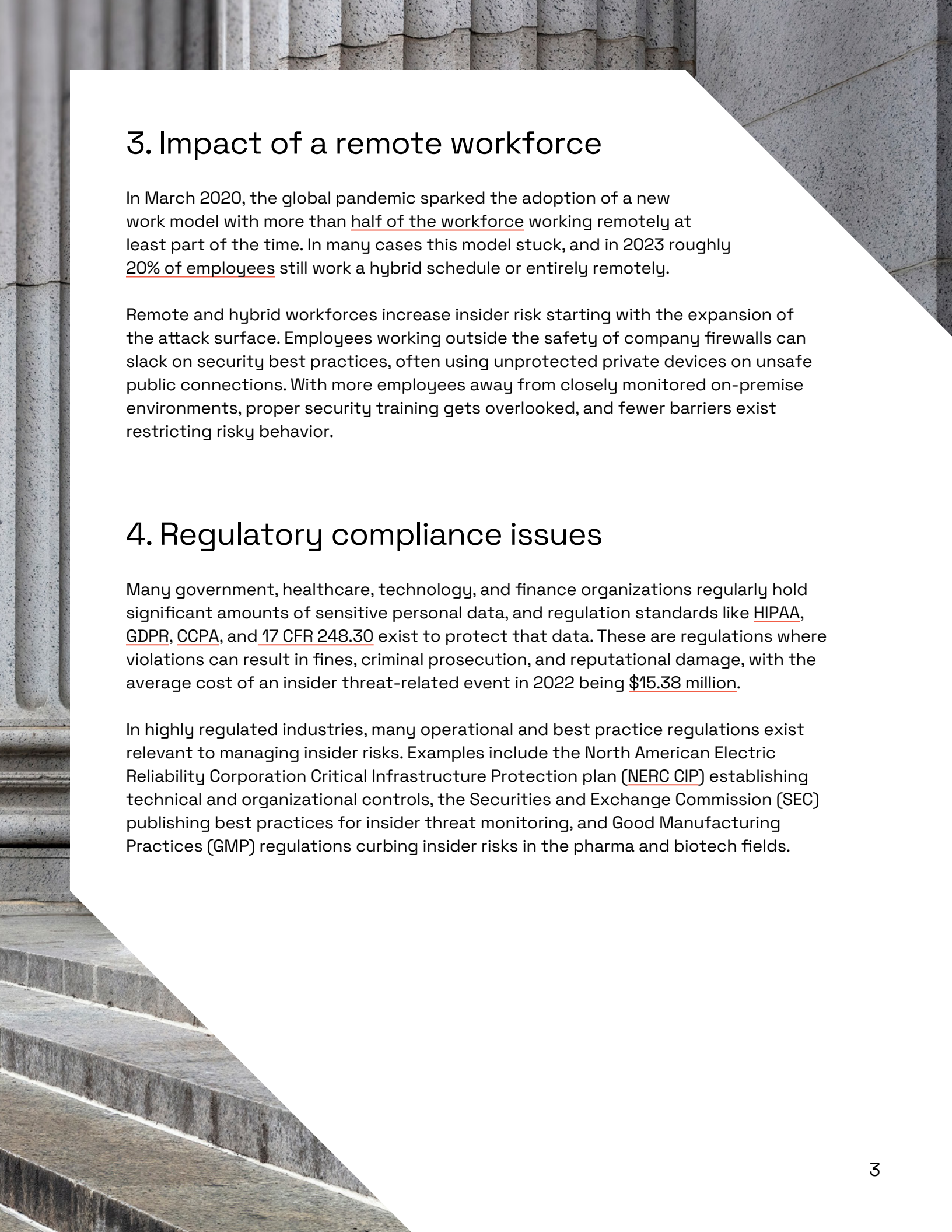
Malicious action is intentional and often driven by a desire for personal gain or vengeance. It can be on the part of an outside attacker who uses social engineering techniques like phishing and malware links to infiltrate the victim's network. Malicious intent can also come from an insider working alone or collaborating with outside fraudsters to steal from or sabotage organizational systems or fellow employees.

Negligence is usually accidental, resulting from convenience or incompetence on the part of an employee who's possibly trying to follow policy but lacks the training to properly perform a function. Negligence can still create dangerous risks, and some examples of negligence include weak passwords, overlooking security best practices, and failing to recognize software updates.

2. Impact of the Great Resignation

In the spring of 2022, a concerning trend appeared regarding employment numbers. Employees were quitting, and at the peak of the Great Resignation, 4.5 million workers per month–3% of all US employees–were leaving their jobs. Many of these vacated positions were in high-regulation industries like healthcare, technology, government, and the financial sector.

Employees leaving can be a significant source of insider risk due to actions required when offboarding personnel. Always remember to follow proper offboarding protocols when someone leaves a position, such as removing their access and credentials and making sure they return company equipment to prevent system vulnerabilities.



3. Impact of a remote workforce

In March 2020, the global pandemic sparked the adoption of a new work model with more than half of the workforce working remotely at least part of the time. In many cases this model stuck, and in 2023 roughly 20% of employees still work a hybrid schedule or entirely remotely.

Remote and hybrid workforces increase insider risk starting with the expansion of the attack surface. Employees working outside the safety of company firewalls can slack on security best practices, often using unprotected private devices on unsafe public connections. With more employees away from closely monitored on-premise environments, proper security training gets overlooked, and fewer barriers exist restricting risky behavior.

4. Regulatory compliance issues

Many government, healthcare, technology, and finance organizations regularly hold significant amounts of sensitive personal data, and regulation standards like HIPAA, GDPR, CCPA, and 17 CFR 248.30 exist to protect that data. These are regulations where violations can result in fines, criminal prosecution, and reputational damage, with the average cost of an insider threat-related event in 2022 being $15.38 million.

In highly regulated industries, many operational and best practice regulations exist relevant to managing insider risks. Examples include the North American Electric Reliability Corporation Critical Infrastructure Protection plan (NERC CIP) establishing technical and organizational controls, the Securities and Exchange Commission (SEC) publishing best practices for insider threat monitoring, and Good Manufacturing Practices (GMP) regulations curbing insider risks in the pharma and biotech fields.

5. Impact on supply chains

It may be an unnerving thought for some, but your organization is only as secure as every entity with which you do business. Any malicious or negligent action within your supply chain or partners, contractors, or vendors can create vulnerabilities, and once inside an organization criminals can move vertically up or down a supply chain.

Encourage every link in your business's supply chain to prioritize educating their employees and providing the threat awareness training necessary to minimize insider risks while increasing their overall cyber hygiene.

6. Impact on public relations

When the news of a successful attack gets out, your organization can expect possible penalties and fines, but that's often not the worst of the fallout. Invaluable customer trust and loyalty can be lost forever when customers have reason to doubt your business's ability to protect their data. Sadly, all it takes is one slip to forever stain your brand in the public eye, permanently damaging your company's reputation.

Dealing with the damage and undergoing recovery can be harsh. 2022 data showed that publicly traded companies suffered an average drop of 7.5% in their stock values after news of a breach, and it reportedly took 46 days, on average, for those stock prices to return to their pre-breach levels—for those lucky enough to recover.

7. Organizational governance is ground zero

Today, managing insider risks is undoubtedly challenging for all organizations, regardless of industry. However, your team can effectively manage insider risks at an organizational level by establishing proper policies and governance early on.

Organizational governance includes setting up a foundation of strict security policies backed by the educational training programs necessary to prepare employees to effectively manage insider risks on all levels of an enterprise.

8. Monitoring isn't the only answer

Monitoring for insider threats is necessary, but companies shouldn't always assume malicious intent. Hyper-monitoring of employees can become counterproductive, fostering a policing culture, building resentment, undermining employee trust and morale, and possibly exceeding the proportionality required by privacy regulations.

Additionally, tracking and reporting every employee action creates an impossible data overload. Organizations should focus on selective monitoring with effective behavioral analytics, creating meaningful alerts emphasizing data quality rather than quantity.

9. Training is critical

Maintaining continuous insider risk training programs can provide a proactive, engaging and more positive approach to countering the growing threat of insider risks. Training focuses on preparing your team to achieve collaborative solutions rather than using scare tactics intended to force compliance.

Robust training programs ensure managers and supervisors can effectively listen, respond, and support employees to disrupt the critical pathways of insider risk.

10. The right tools can help differentiate between malicious and negligent events after an incident

After a security incident involving an insider, it's crucial to understand what occurred, determine motivation and intent, and take appropriate action. This may sometimes involve removing a malicious inside collaborator, quickly identifying and patching a vulnerability, or re-training an innocent but negligent employee in order to prevent a repeat performance.

Data analysis tools focusing on quality over quantity from a security partner like Everfox can help organizations quickly understand a security incident. These tools provide accurate, consumable breakdowns so your team can correctly support well-meaning employees or identify malicious perpetrators based on factual data, when getting the right answers fast matters most.

EVERFOX

Everfox has been defending the world's critical data and networks against complex cyber threats for more than 25 years. As trailblazers in defense-grade, high-assurance cybersecurity, Everfox has led the way in delivering and developing innovative cybersecurity technology. Headquartered in Herndon, VA, Everfox's suite of Cross Domain, Threat Protection and Insider Risk Solutions empower governments and enterprise organizations to use data safely — wherever and however their people need it.

Learn More